CHAPTER IX

CONTINUING SECURITY RESPONSIBILITIES

Section 1

Evaluating Continued Security Eligibility

9-100 General

A. personnel security determination is an effort to assess the future trustworthiness of an individual in terms of the likelihood of the individual preserving the national security. Obviously it is not possible at a given point to establish with certainty.. that any human. being will remain trustworthy. Accordingly, the issuance of a personnel security clearance or the determination that a person is suitable for assignment to sensitive duties cannot be considered as a final personnel security action. Rather, there is the clear need to assure that, after the personnel security determination is reached, the individual's trustworthiness is a matter of continuing assessment. The responsibility for such assessment must be shared by the organizational commander or manager, 'the individual's supervisor and, to a large degree, the individual himself. Therefore, the heads of DoD Components shall establish and maintain a program designed to evaluate on a continuing basis the status of personnel under their jurisdiction with respect to security eligibility. This program should insure close coordination between security authorities and personnel, medical, legal and supervisory personnel to assure that all pertinent information available within a command is considered in the personnel security process.

9-101 Management Responsibility

a. Commanders and heads of organizations shall insure that personnel assigned to sensitive duties (or other duties requiring a trustworthiness determination under the provisions of this Regulation) are initially indoctrinated and periodically instructed thereafter on the national security implication of their duties and on their individual responsibilities.

b. The heads of all DoD components are encouraged to develop programs designed to counsel and assist employees in sensitive positions who are experiencing problems in their personal lives with respect to such areas as financial, medical or emotional difficulties. Such initiatives should be designed to identify potential problem areas at an early stage so that any assistance rendered by the employing activity will have a reasonable chance of precluding long term, job-related security problems.

9-102 Supervisory Responsibility

Security programs shall be established to insure that supervisory personnel are familiarized with their special responsibilities in matters pertaining to personnel security with respect to personnel under their supervision. Such programs shall provide practical guidance as to indicators that may signal matters of personnel security concern. Specific instructions should

be disseminated concerning reporting procedures to enable the appropriate authority to take timely corrective action to protect the interests of national security as well as to provide any necessary help to the individual concerned to correct any personal problem which may have a bearing upon the individual's continued eligibility for access.

a. In conjunction with the submission of PRs stated in Section 7, Chapter III, and paragraph 5, Appendix B, supervisors will be required to review an individual's DD Form 398 to ensure that no significant adverse information of which they are aware and that may have a bearing on subject's continued eligibility for access to classified information is omitted.

b. If the supervisor is not aware of any significant adverse information that may have a bearing on the subject's continued eligibility for access, then the following statement must be documented, signed and dated, and forwarded to DIS with the investigative package.

"I am aware of no information of the type contained at Appendix E, DoD 5200.2-R, relating to subject's trustworthiness, reliability, or loyalty that may reflect adversely on his/her ability to safeguard classified information."

c. If the supervisor *is* aware of such significant adverse information, the following statement shall be documented, signed and dated and forwarded to DIS with the investigative package, and a written summary of the derogatory information forwarded to DIS with the investigative package:

"I am aware of information of the type contained in Appendix E, DoD 5200.2-R, relating to subject's trustworthiness, *reliability, or* loyalty that may reflect adversely on his/her ability to safeguard classified information and have reported all relevant details to the appropriate security official(s)."

d. In conjunction with regularly scheduled fitness and performance reports of military and civilian personnel whose duties entail access to classified information, supervisors will include a comment in accordance with paragraphs 9-102 b. and c., above, as well as a comment regarding an employee's discharge of security responsibilities, pursuant to their Component guidance.

9-103 Individual Responsibility

a. Individuals must familiarize themselves with pertinent security regulations that pertain to their assigned duties. Further, individuals must be aware of the standards of conduct required of persons holding positions of trust. In this connection, individuals must recognize and avoid the kind of personal behavior that would result in rendering one ineligible for continued assignment in a position of trust. In the final analysis, the ultimate responsibility for maintaining continued eligibility for a position of trust rests with the individual.

b. Moreover, individuals having access to classified information must report promptly to their security office:

(1) Any form of contact, intentional or otherwise, with a citizen of a designated country, (appendix H) unless occurring as a function of one's official duties.

(2) Attempts by representatives or citizens of designated countries to cultivate friendships or to place one under obligation.

(3) Attempts by representatives or citizens-of foreign countries to:

(a) Cultivate a friendship to the extent of placing one under obligation that they would not normally be able *to* reciprocate, or by offering money payments or bribery to obtain information of actual or potential intelligence value.

(b) Obtain information of actual or potential intelligence value through observation, collection of documents, or by personal contact.

(c) Coerce by blackmail, by threats against or promises of assistance to relatives living under foreign control, especially those living in a designated country.

(4) All personal foreign travel in advance.

(5) Any information of the type referred to in paragraph 2-200 *or* Appendix I.

9-104 Co-worker Responsibility

Co-workers have an equal obligation to advise their supervisor or appropriate security official when they become aware of information with potentially serious security significance regarding someone with access to classified information or employed in a sensitive position.

Section 2

SECURITY EDUCATION

9-200 General

The effectiveness of an individual *in* meeting security responsibilities is proportional to the degree to which the individual understands them. Thus, an integral part of the DoD security program is the indoctrination of individuals on their security responsibilities. Moreover, such indoctrination is essential to the efficient functioning of the DoD personnel security program. Accordingly, heads of DoD Components shall establish procedures in accordance with this chapter whereby persons requiring access to classified information, or being assigned to positions that require the occupants to be determined trustworthy are periodically briefed as to their security responsibilities.

9-201 Initial Briefing

a. **All persons cleared for access to classified information *or* assigned to duties requiring a trustworthiness determination under this Regulation shall be given an initial security briefing. The briefing shall** be in accordance **with the requirements of paragraph 10-102, DoD 5200.1-R** (reference (q)) and consist of the following elements:

(1) The specific security requirements of their particular job.

(2) The techniques employed by foreign intelligence activities in attempting to obtain classified information and their responsibility for reporting such attempts.

(3) The prohibition against disclosing classified information, **by any means, to unauthorized persons** or discussing or handling classified information in a manner that would make **it accessible to unauthorized persons.**

(4) The penalties that may be imposed for security violations.

b. **If an individual declines to execute Standard Form 189, "Classified Information Nondisclosure Agreement," the DoD Component shall initiate action to deny or revoke the security clearance of such person in accordance with paragraph 8-201, above.**

9-202 Refresher Briefing

Programs shall be established to provide, at a minimum, annual security *training for* personnel having *continued access to classified* information. **The elements outlined in paragraph 10-101, DoD 5200.1-R (reference (q)) shall be tailored to fit the needs of experienced personnel.**

9-203 Foreign Travel Briefing

a. **DoD Components will establish appropriate internal procedures requiring all personnel possessing a DoD security clearance to report to their security office all personal *foreign travel in* advance of the travel being performed. When travel patterns, or the failure to report such travel, indicate the need for investigation, the matter will be referred to the appropriate counterintelligence investigative agency.**

b. **Personnel having** access **to classified information shall be given a Foreign Travel Briefing by a counterintelligence agent, security specialist, security manager, or other qualified individual, as a defensive measure prior to travel to a designated country (Appendix H) *in order to* alert *them to* their possible exploitation by hostile intelligence services. These personnel will also be debriefed upon their return. The briefings will be administered under the following conditions:**

(1) Travel to or through a designated country for any purpose.

(2) Attendance at international, scientific. technical, *engineering,* **or other professional meetings in the United States or in any country**

outside the United States when it can be anticipated that representative(s) of designated countries will participate or be in attendance.

c. Individuals who travel frequently, or attend or host meetings of foreign visitors as described in b.2., above, need not be briefed for each occasion, but shall be provided a through briefing at least once every 6 months and a general reminder of security responsibilities before each such activity.

d. Records on such employees will be maintained for 5 years.

9-204 Termination Briefing

a. Upon termination of employment administrative withdrawal of security clearance, or contemplated absence from duty or employment for 60 days or more, DoD military personnel and civilian employees shall be given a termination briefing, return all classified material, and execute a Security Termination Statement. This statement shall include:

(1) An acknowledgment that the individual has read the appropriate provisions of the Espionage Act, other criminal statutes, DoD Regulations applicable to the safeguarding of classified information to which the individual has had access, and understands the implications thereof;

(2) A declaration that the individual no longer has any documents or material containing classified information in his or her possession;

(3) An acknowledgment that the individual will not communicate or transmit classified information to any unauthorized person or agency; and

(4) An acknowledgment that the individual will report without delay to the FBI or the DoD Component *concerned* any attempt by any unauthorized person to solicit classified information.

b. When an individual refuses to execute a Security Termination Statement, that fact shall be reported immediately to the security manager of the cognizant organization concerned. In any such case, the individual involved shall be debriefed orally. The fact of a refusal *to sign a Security* Termination Statement shall be reported to the Director, Defense Investigative Service who shall assure that it is recorded in the Defense Central Index of Investigations.

c. The Security Termination Statement shall be retained by the DoD Component that authorized the individual access to classified information for the period specified in the Component's records *retention* schedules, but for a minimum of 2 years after the individual is given a termination briefing.

d. In addition to the provisions of subparagraphs a., b., and c. above, DoD Components shall establish a central authority to be responsible for ensuring that Security Termination Statements are executed by senior personnel (general officers, flag officers and GS-16s and above). Failure on the part of such personnel to execute a Security Termination Statement shall be reported immediately to the Deputy Under Secretary of Defense for Policy.